Y

Yontoo Adware: Detection Meaning, Removal, and Browser Repair

Yontoo is a detection name associated with adware and browser-hijacking components. The detection path helps distinguish an old installer from active software.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

Yontoo is a name associated with adware and browser-modification software distributed through bundled installers and extensions. Security vendors may use labels such as **Adware.Yontoo** for a broad family rather than one identical file.

Malwarebytes currently describes Adware.Yontoo as a generic detection for Windows adware with browser-hijacking capabilities, while F-Secure documents historical macOS Yontoo extensions. Use the operating system, detection path, file hash, and security-vendor description to interpret the alert.

What the detection location means

- **Downloads or archive:** the bundled installer may have been detected before execution.
- **Installed application folder:** an active or previously installed component may remain.

- **Browser profile or extension:** review the extension and any account sync that can restore it.
- **Backup or quarantine:** the item may be inactive but should not be restored or copied to another system.

Possible symptoms

- new advertisements injected into normally clean pages;
- search, homepage, or new-tab changes;
- redirects through unfamiliar advertising domains;
- an unknown extension, toolbar, updater, proxy, profile, or startup component;
- the browser setting returns after manual repair.

Ads alone do not prove Yontoo. Website advertising, malicious notifications, and other adware can look similar. Confirm the local detection and source.

Removal steps

1. **Record the alert.** Save the path, detection name, action, publisher, and related installation date.
2. **Quarantine the detected item.** Delete the original unofficial installer or archive after preserving what an administrator needs for investigation.
3. **Uninstall related applications.** Use normal system settings and review other programs installed on the same date.
4. **Repair browsers.** Remove unknown extensions, notification permissions, search providers, startup pages, and managed policies. Check every profile and browser.
5. **Review system settings.** Inspect proxy, DNS, startup entries, scheduled tasks, login items, and configuration profiles when redirects affect more than one browser.

6. **Scan again after restart.** A returning detection can point to a helper, sync account, another user profile, or restore location.

Avoid copying old manual file lists from unrelated variants. Deleting the wrong profile, registry value, or system component can damage legitimate software without removing the source.

On a managed device, export browser policy and extension inventory before resetting profiles. An organization-wide policy, software deployment package, or shared browser account can affect several machines, so repeated detections should be investigated centrally instead of fixed one endpoint at a time.

If redirects captured information

From a clean device, change credentials entered on a redirected page, revoke sessions, and review MFA and recovery settings. Contact the bank or card issuer if payment data was exposed. Yontoo is primarily an adware label, but malicious advertisements can lead to separate phishing or malware incidents.

Prevention

- download from official publishers and trusted stores;
- reject optional offers in custom installation;
- keep PUA protection enabled;
- limit extensions and review browser sync periodically;
- avoid download wrappers, fake video tools, cracks, and update popups.

Yontoo FAQ

Is Yontoo still active malware?

A present alert can be an active component, generic family match, or old artifact. The path and execution evidence determine urgency.

Is resetting the browser enough?

Not when an installed helper, policy, sync account, proxy, or DNS setting recreates the change.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com